DATA PROTECTION POLICY

1 DATA PROTECTION

1.1 C R Encapsulation Limited (the **"Company"**) (company number SC228211) recognises the importance of respecting the personal privacy of all employees and also the need to put in place appropriate safeguards surrounding the collection, destruction, storage, processing and utilisation of personal data.

1.2 The aim of the Company is to ensure that personal data is obtained, stored, processed, used, disclosed and destroyed in accordance with the data protection principles set out in the General Data Protection Regulation (the **"GDPR"**) and related data protection legislation (collectively the **"Data Protection Legislation"**), and the purpose of this data protection policy (the **"Policy"**) is to establish internal procedures to manage our compliance with these requirements.

1.3 The Policy sets out:

1.3.1 the general requirements that are applicable to you in handling personal information in the course of your work with the Company; and

1.3.2 information concerning what personal information the Company holds, where it is obtained from and how it is used.

1.4 Please read this Policy carefully and make sure that you understand and comply with all the rules, as failure to comply may, depending on the violation, result in disciplinary action, including dismissal, and the Company may also inform and involve the appropriate authorities.

1.5 The Finance Director (the **"Appointed Representative"**) is responsible for co-ordinating the Company's overall compliance with the requirements of the Data Protection Legislation. If you consider that this Policy has not been followed in respect of your personal data or the personal data of others, or if you become aware of a data security breach, you should raise the matter with the Appointed Representative.

1.6 This policy applies to all individuals working at all levels and grades, and in all departments of the Company. In addition to this, the Policy also applies to:

1.6.1 Temporary employees (including those on work experience);

1.6.2 Agency employees; and

1.6.3 Suppliers, including independent contractors and subcontractors who will have access to personal data belonging to the company as required for the delivery of the services.

2 DATA PROTECTION RULES

2.1 The purpose of Data Protection Legislation is to safeguard information held about individuals.

2.2 For the purposes of this Policy, the Company is the data controller for all personal data collected and used in its business for its own purposes. The Company has notified the Information Commissioner's Office that it is a data controller under registration number ZA031512.

2.3 The Company may require to transfer your personal data to another entity within the Company's group for its own business purposes.

2.4 **Personal Data**

2.4.1 Data protection rules are concerned with 'personal data', that is information held on any living individual which, on its own or in conjunction with other information held by the Company, directly or indirectly identifies that individual. It includes expressions of opinion or intention and manual or computerised records.

2.4.2 The Company collects, stores and processes personal data about various groups of people including employees, clients, agents, suppliers and other third parties.

2.4.3 The types of data collected, stored and processed may include but not be limited to: contact details, bank accounts, date of birth, marital status etc.etc.

2.5 **The Company's Obligations**

In this respect it must adhere to the following data protection principles (the **"Principles"**) in accordance with the GDPR:

Personal data shall be:

2.5.1 processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2.5.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

2.5.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

2.5.4 accurate and, where necessary, be kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay ('accuracy');

2.5.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation'); and

2.5.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2.6 **Purpose for processing personal data**

The Company will only obtain, store and use personal data for legitimate business purposes and / or where there is a statutory or contractual requirement to do so. These purposes include:

2.6.1 Recruitment and employment (including post-employment management);

2.6.2 Conducting the everyday business of the Company;

2.6.3 Advertising and marketing the services of the Company;

2.6.4 Compliance with the legislation that applies to the Company, including health and safety;

2.6.5 Working with the relevant authorities to investigate breaches of the law, including crime and fraud;

2.6.6 Addressing and investigation of complaints, grievances and claims;

2.6.7 Paying employees;

2.6.8 Providing employees with certain benefits;

2.6.9 Using a CCTV system to monitor and collect visual images for the purpose of security and the prevention and detection of crime;

2.6.10 Driving licence checks;

2.6.11 Insurance claims; and

2.6.12 Training records.

2.7 Should the Company require to process personal data for any other purpose, it shall notify the relevant individuals in advance of doing so.

2.8 The Company does not use data for automated decision-making.

2.9 **Sensitive Personal Data**

2.9.1 Extra care should be taken with any personal data that is classed as "sensitive" (also known as "special categories" of personal data). Information is classed as sensitive personal data if it relates to the following: (i) racial or ethnic origin; (ii) political opinions; (iii) religious or similar beliefs; (iv) trade union membership; (v) physical or mental health condition; (vi) sexual life; (vii) commission or alleged commission of an offence; (viii) any court proceedings or findings; and (ix) genetic and biometric data.

2.9.2 The Company may hold sensitive personal data about its employees for occupational health purposes and to ensure compliance with equal opportunities legislation.

2.10 The Company shall process personal data for as long as is necessary to fulfil the purposes it collected it for as provided for in section 2.6, in accordance with applicable laws. To determine the appropriate retention period for personal data, the Company considers the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which it processes personal data and whether it can achieve those purposes through other means, and the applicable legal requirements. Personal data destroyed or deleted will be done so in accordance with the Company Data Retention Policy.

2.11 If you fail to provide certain information when requested, the Company may not be able to perform the contract entered into with you (such as paying you or providing a benefit), or the Company may be prevented from complying with its legal obligations (such as to ensure the health and safety of our workers).

3 HOW THE LAW CAN AFFECT YOU

3.1 As an individual you will be a 'data subject' (an individual about whom personal data is held by the Company).

3.2 As an employee:

3.2.1 You are responsible for ensuring that Data Protection Legislation is followed.

3.2.2 Take sensible and reasonable precautions to protect information in your care.

3.2.3 Observe any instructions or guidelines issued by the Company in relation to data protection and your work.

3.2.4 Observe the Principles at all times.

3.2.5 Always ensure that data is inputted correctly. Do not delay in inputting new data when available.

3.2.6 Do not make any oral or written reference to personal data held by the Company about any individual except to employees of the Company who need the information for their work or a registered recipient.

3.2.7 Take great care to establish the identity of any person asking for personal information. Make sure that the person is entitled to receive the information.

3.2.8 If you are asked by an individual to provide details of their personal information held by the Company, you should ask that they put their request in writing and send it to the Authorised Representative.

3.2.9 Do not use personal information for any purpose other than your work for the Company.

3.2.10 Take confidentiality and security seriously whether you consider the information to be sensitive or not. In particular:

- do not disclose your password;
- if personal information is kept on manual files ensure that they are kept in a locked filing cabinet or drawer;
- change your password regularly;
- do not gossip about Company data;
- do not leave Company data in any public place, such as the street, on the train, or on the bus etc.;
- do not take computer scrap paper home;
- do not allow unauthorised use of computer equipment issued by the Company; and
- take care to ensure that client confidential information is sent securely to the intended recipient.

3.3 If you are in doubt about any matter to do with data protection, do not guess - refer the matter to the Authorised Representative immediately.

4 RIGHTS OF INDIVIDUALS

4.1 The Company recognises that data protection rules provide rights to the individuals whose personal data it processes. These rights include:

4.1.1 the right to access personal data the Company holds about them;

4.1.2 the right to know why their personal data is being processed;

4.1.3 the right to have their personal data deleted;

4.1.4 the right to request certain personal data is restricted from processing where there is a question as to its accuracy, the processing is unlawful, there is no need to process the personal data or there is an objection to the personal data and the decision is pending;

4.1.5 the right to request certain personal data transferred to a third party;

4.1.6 the right to withdraw consent to the personal data being processed (where consent is actually relied upon);

4.1.7 the right to complain to the authoritative body (e.g. the Information Commissioner's Office in the United Kingdom), further details below at section 5; and

4.1.8 the right to understand any consequences of not giving data.

The Company shall, at all times, adhere to any rights of an individual under the data protection rules. Should you wish to exercise any of the above rights, please contact the Authorised Representative.

5 COMPLAINTS

If you have any questions about this Policy or how the Company handles your personal information, please contact the Authorised Representative. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

6 TRANSFERS OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

6.1 If the Company transfers your data outside the European Economic Area, it will take steps to ensure that appropriate security measures and safeguards are in place with the aim that your rights continue to be protected as set out in this Policy. This shall include ensuring adequate protection is in place as required by applicable data protection law.

6.2 If you are required by your role to transfer data outside of the European Economic Area, please discuss this with the Authorised Representative.

7 CHANGES TO PERSONAL DETAILS

7.1 The Company is required to maintain accurate records of the personal data it processes. Accuracy of personal data shall be checked at regular intervals.

7.2 To assist the Company with its obligation to maintain accurate records, if you change your name, address, marital status, or other personal details, please notify the Authorised Representative immediately.

7.3 Fraudulent claims relating to personal details will result in disciplinary action, which may lead to dismissal.

8 USE OF LAPTOP COMPUTERS AND MOBILE DEVICES

Where employees are in receipt of computer equipment or mobile devices issued by the Company to assist in their day-to-day work, then you must adhere to the data protection principles and Acceptable Use Policy. Particular care should be taken to ensure the security of data when using mobile devices on unsecured networks.

9 CONFIDENTIALITY AND SECURITY AT WORK

9.1 The Company must ensure, at all times, that appropriate technical and organisational security measures are taken against the unlawful or unauthorised processing or disclosure of personal data, and against the accidental loss of, or damage to, personal data.

9.2 In the course of your work you will have access to information of a personal or financial nature. Employees must remember that the information is confidential and must not be passed to anyone else outside of the Company.

9.3 Employees should abide by the following security procedures to ensure appropriate security measures are followed:

9.3.1 any stranger seen in an entry-controlled areas should be reported;

9.3.2 desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential);

9.3.3 paper documents which contain personal information should be shredded, and CD-ROMs or USBs which contain personal information should be physically destroyed when they are no longer required; and

9.3.4 employees should ensure that individual PC monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.

9.4 Falsifying Company documents (including computer held data) whether or not for personal gain will be treated as gross misconduct and may lead to disciplinary action and the Company may inform and involve the appropriate authorities.

10 CONTACT

If you have any questions, concerns or complaints about the interpretation or operation of this policy please discuss these with Authorised Representative –

Joe Murdoch
Finance Director
CR Encapsulation Ltd
Bourtree Complex
Minto Drive
Altens Industrial Estate
ABERDEEN
AB12 3LW

joe@cre-marine.com

R MAIR
Managing Director
3 September 2019

Next review date: 2 September 2020